Information Security Policy

Montague Independent School District

Purpose:

The purpose of the information security policy is:

- To establish a district-wide approach to information security and data loss prevention.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of Montague ISD'S data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of the Montague ISD and allow the Montague ISD to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

Montague ISD will apply policies, procedures, practice standards, and guidelines to protect its IT functions from internal data or programming errors and from misuse by individuals within or outside the Montague ISD. This is to protect the Montague ISD from the risk of compromising the integrity of shared data, violating individual rights to privacy and confidentiality, violating criminal law, or potentially endangering the public's safety.

Data privacy is clearly defined as the appropriate use of data. When Montague ISD's data and information is provided and entrusted to them, the data will be used according to the agreed purposes.

All Montague ISD's information security programs will be responsive and adaptable to changing technologies affecting information resources. In addition, Montague ISD will strive to identify and adhere to all security compliance and regulatory requirements set forth by the State as well as the federal government including but not limited to:

1. Family Education Rights and Privacy Act (FERPA) - Under this regulation, families have the right to request their child's education records and they have the right to submit those requests via email or an online submission form. Montague ISD is required to reply to those requests.

2. The Protection of Pupil Rights Amendment - This regulation protects minor students from disclosing personal information if they or their parents do not wish to disclose the information in question. This extends to electronic surveys, polls or other questionnaires. Under the Protection of Pupil Rights Amendment regulation, Montague ISD must get consent from parents before asking children about specific personal information.

3. The Freedom of Information Act - This regulation applies specifically to public schools. As government institutions, Montague ISD is required to respond to requests for information. Under this act, Montague ISD must make available copies of all records, regardless of format. That includes emails, blog posts, and more.

4. The Americans with Disabilities Act – this act extends to Montague ISD's website. The district's website is the online proxy for our school, and disabled students and parents need to have access to it just all other members of your community do. This especially applies to screen readers, which are often used by individuals with poor vision. Montague ISD's website will be designed in such a way that it is easy for a screen reader to scan for disabled students and/or parents.

Ownership:

The Information Security Policies are owned by the Montague ISD's Information Resources Manager (IRM). The IRM, or designate, is the only authority that can approve modifications to the Security Policies.

These Policy Standards apply equally to all personnel including, but not limited to, Montague ISD's employees, agents, consultants, volunteers, and all other authorized users granted access to information resources.

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of Montague ISD's information resources access privileges, as well as civil and criminal prosecution.

Policy Development and Maintenance:

Montague ISD's Information Security Policies provide the operational detail required for the successful implementation of the Information Security Program. These security policies were developed based on, and cross referenced to, the Security Policy Standards. In addition, these policies have been developed by interpreting Health Insurance Portability and Accountability Act of 1996 (HIPAA), Texas Administrative Code, Chapter 202 (TAC 202) and other legislation and legal requirements, understanding business needs, evaluating existing technical implementations, and by considering the cultural environment.

The business, technical, cultural, and legal environment of Montague's ISD, as it relates to information resources use and security, is constantly changing. These policies are technology neutral and apply to all aspects of information resources. Emerging technologies or new legislation, however, will impact these Information Security Policies over time. The Security Policies will be revised as needed to comply with changes in federal or state law or rules promulgated there under or to enhance its effectiveness.

A number of factors could result in the need or desire to change the Security Policies. These factors include, but are not limited to:

- Review schedule
- New federal or state legislation
- Newly discovered security vulnerability
- New technology
- Audit report
- Business requirements
- Cost/benefit analysis
- Cultural change

Updates to the Montague ISD's Information Security Policies, which include establishing new policies, modifying existing policies, or removing policies, can result from three different processes:

- At least annually, the Information Security Officer (ISO), or designee, will review the Policies for possible addition, revision, or deletion. An addition, revision, or deletion is created if it is deemed appropriate.

- Every time new information resource technology is introduced into the Montague ISD, a security assessment should be completed. The security assessment or technology risk assessment will help identify risks from the use of technology that could potentially cause information loss or financial or reputational harm to Montague ISD or operational distribution to the district's technology network or programs. During this assessment, four IT security objectives: confidentiality, data integrity, availability, and authorized use will be evaluated and will be identified as at low, moderate, or high risk. The result of the security/technology risk assessment could necessitate changes to the Security Policies before the new technology is permitted for use at Montague ISD.

Any User may propose the establishment, revision, or deletion of any practice standard at any time. These proposals should be directed to the ISO who will evaluate the proposal and make recommendations to the Information Resource Manager (IRM).

Once a change to the Security Policies has been approved by the IRM, or designee, the following steps will be taken as appropriate to properly document and communicate the change:

- The appropriate IT Security web pages will be updated with the change
- Training and compliance materials will be updated to reflect the change

The changes will be communicated using standard Montague ISD's communications methods such as: announcements, web page notification, newsletters, and communications meetings.

Key Roles & Responsibilities Including Oversight/Governance/Safeguard Assurance:

Information Resources Manager (IRM): Responsible for the Montague ISD and the State of Texas for management of the Montague ISD's information resources. The designation of Montague ISD's IRM is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state of Montague ISD's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the information resources of Montague ISD.

Information Security Officer (ISO): Angela Kleinhans, responsible to the IRM for administering the information security function within Montague ISD. The ISO is the Montague ISD's internal and external point of contact for all information security matters. The ISO duties include but are not limited to:

- Assuring the information security policy is updated on a regular basis (at a minimum annually) and published as appropriate.
- Providing appropriate training is provided to data owners, data custodians, network and system administrators, and users.
- Appointing a person, if applicable, to be responsible for security implementation, incident response, periodic user access reviews, and education of information security policies including, for example, information about virus infection risks.

Technology Management Team (TMT): Angela Kleinhans, Carla Hennessey, Staley Keck, Jesse Romine- designated as a coordinating group comprised of information personnel from the Montague ISD, chaired by the IRM and chartered with the task to establish procedures to implement these policies within their areas of responsibility and for monitoring compliance.

Program Manager: Angela Kleinhans assigned information resource ownership; responsible for the information used in carrying out program(s) under their direction and provides appropriate direction to implement defined security controls and procedures.

Technical Manager (TM): Angela Kleinhans, assigned custodians of information resources; provide technical facilities and support services to owners and users of information. TM's assist Program Management in the selection of cost-effective controls used to protect information resources. TM's are charged with executing the monitoring techniques and procedures for detecting, reporting, and investigating breaches in information asset security.

Owner: Angela Kleinhans, the manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is

responsible for establishing the controls that provide security. The owner of a collection of information is the person responsible for the business results of that system or the use of the information. Where appropriate, ownership may be shared by managers of different departments.

Custodian: Angela Kleinhans- guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For server applications Information Technology is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

User: Angela Kleinhans- has the responsibility to (1) use the resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user is the single most effective control for providing adequate security.

Information Technology (IT): Angela Kleinhans, Jesse Romine

Internal Auditor: Angela Kleinhans- ensures that the Montague ISD's information resources are being adequately secured, based on risk management, as directed by the IRM acting on delegated authority for risk management decisions.

System Administrator: Angela Kleinhans person responsible for the effective operation and maintenance of information resources, including implementation of standard procedures and controls to enforce an organization's security policy. Technical management may designate a number of system administrators.

Security Awareness and Training:

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously upgraded and reinforced. Montague ISD guidelines are as follows:

- All users must sign an acknowledgement stating they have read and understand Montague ISD's requirements regarding computer security policies and procedures.
- All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect Montague ISD's information resources.
- IT must prepare, maintain, and distribute one or more information security manuals that concisely describe Montague ISD's information security policies and procedures.
- IT must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest as approved by the ISO.

Policy Standards:

1. Information Technology Security controls must not be bypassed or disabled.
2. Security awareness of personnel must be continually emphasized, reinforced, updated and validated.
3. All personnel are responsible for managing their use of information resources and are accountable for their actions relating to information resources security. Personnel are also equally responsible for

reporting any suspected or confirmed violations of this policy to the appropriate management immediately.

4. Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner department management immediately.

5. Access to, change to, and use of information resources must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as at each job status change such as: a transfer, promotion, demotion, or termination of service.

6. The use of information resources must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of information resources utilization, the establishment of effective use, and reporting of performance to management.

7. Any data used in an information resources system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore, if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.

8. All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property.

9. On termination of the relationship with the Montague ISD users must surrender all property and information resources managed by Montague ISD. All security policies for information resources apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.

10. The owner must engage the IRM, or designate, at the onset of any project to acquire computer hardware or to purchase or develop computer software. The costs of acquisitions, development and operation of computer hardware and applications must be authorized by appropriate management. Management and the requesting department must act within their delegated approval limits in accordance with the Montague ISD'S authorization policy. A list of standard software and hardware that may be obtained without specific, individual approval will be published.

11. The department which requests and authorizes a computer application (the owner) must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired for, computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the custodian.

12. The information resource network is owned and controlled by IT. Approval must be obtained from IT before connecting a device that does not comply with published guidelines to the network. IT reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.

13. The sale or release of computer programs or data, including email lists and departmental telephone directories, to other persons or organizations must comply with all Montague ISD'S legal and fiscal policies and procedures.

14. The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.

15. All changes or modifications to information resource systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.

16. Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.

17. All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the Montague ISD'S is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

18. Montague ISD's disaster recovery procedures include the following: MISD contracts with PCNET to assist in the recovery process of lost data.

19. All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized Montague ISD officer and must contain terms approved as to form by the Legal Department.

20. Information resources computer systems and/or associated equipment used for Montague ISD business that is conducted and managed outside of Montague ISD's control must meet contractual requirements and be subject to monitoring.

21. External access to and from information resources must meet appropriate published ABC ISD security guidelines.

22. All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The IRM through IT reserves the right to remove any unlicensed software from any computer system.

23. Assessment of risk shall guide the selection of media, and associated information contained on

that media requiring restricted access. TMT (Technology Management Team) shall document policies and procedures for the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

24. The IRM through IT reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to: games, instant messengers, pop email, music files, image files, freeware, and shareware.

25. Adherence to all other policies, practice standards, procedures, and guidelines issued in support of these policy statements is mandatory.

Any event that results in theft, loss, unauthorized use, unauthorized disclosure, unauthorized modification, unauthorized destruction, or degraded or denied services of information resources constitutes a breach of security.

Violations may include, but are not limited to any act that:

- exposes the Montague ISD'S to actual or potential monetary loss through the compromise of information resources security,
- involves the disclosure of sensitive or confidential information or the unauthorized use of Montague ISD'S data or resources,
- involves the use of information resources for personal gain, unethical, harmful, or illicit purposes, or results in public embarrassment to the Montague ISD'S.

Violations of these Information Security Policies may result in immediate disciplinary action that may include, but may not be limited to:

- formal reprimand,
- suspended or restricted access to Montague ISD'S information resources,
- restitution or reimbursement for any damage or misappropriation of any Montague ISD'S property,
- suspension without pay,
- termination of employment,
- termination of contract,
- civil prosecution or state and/or federal criminal prosecution.

Ownership of Electronic Files:

Electronic files created, sent, received, or stored on information resources owned, leased administered, or otherwise under the custody and control of Montague ISD and are the property of Montague ISD.

Privacy:

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of Montague ISD are not private and may be accessed by Montague ISD IT employees at any time without knowledge of the information resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. Please refer to Montague ISD's Acceptable Use Policy.

Account Management Policy:

•All accounts created must have an associated request and approval that is appropriate for the Montague ISD system or service.
•All users must sign the Montague ISD Information Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
•All accounts must be uniquely identifiable using the assigned username.
•All default passwords for accounts must be constructed in accordance with Montague ISD's Password Policy.
•All accounts must have a password expiration that complies with Montague ISD's Password Policy.
•Accounts of individuals on extended leave (more than 30 days) will be disabled.
•All new user accounts that have not been accessed within 30 days of creation will be disabled.
•Supervisors are responsible for immediately notifying Information Security of individuals who change roles within ABC ISD or are separated from their relationship with Montague ISD.
•System Administrators or other designated staff:

*are responsible for removing the accounts of individuals that change roles within Montague ISD or are separated from their relationship with Montague ISD

*must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes

*must have a documented process for periodically reviewing existing accounts for validity

*are subject to independent audit review

*must provide a list of accounts for the systems they administer when requested by authorized Montague ISD management

*must cooperate with authorized Montague ISD management investigating security incidents.

Data Classification Policy:

It is essential that all Montague ISD's data be protected. There are, however, gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. To assure proper protection of Montague ISD's information resources, various levels of classifications will be applied. The Montague ISD has specified three classes below:

High Risk/Private - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA or the Data Protection Act, are in this class. Payroll, personnel, and financial information are also in this class because of privacy requirements. This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to Montague ISD if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.

Confidential – Data that would not expose Montague ISD to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.

Public - Information that may be freely disseminated.

All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through Montague ISD.

- Owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.

- No Montague ISD-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- Custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.
- High risk data must be encrypted during transmission over insecure channels. Cryptography will be used to provide secrecy and integrity to Montague ISD's data, and both authentication and anonymity to our communications.
- Confidential data should be encrypted during transmission over insecure channels.
- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted, or disks destroyed consistent with industry best practices for the security level of the data.

Information Security Risk Management:

Information security risk management, or ISRM, is the process of managing the risks associated with the use of information technology. In other words, organizations identify and evaluate risks to the confidentiality, integrity and availability of their information assets. This process can be broadly divided into two components:

*Risk assessment — The process of combining the information you have gathered about assets and controls to define a risk. Montague ISD has identified the following cybersecurity risks to systems, people, assets, data and capabilities: MISD uses a Sonic Wall content filter and all teacher desktops are protected with anti-virus software.
*Risk treatment — The actions taken to remediate, mitigate, avoid, accept, transfer or otherwise manage the risks. Montague ISD has implemented the following safeguards and security controls to protect against cyber threats: firewall(s), antivirus/security software, security updates. Montague ISD will use the following techniques to contain the impact of an incident: response planning, communications, analysis, mitigation and improvements. Lastly, Montague ISD will develop and implement activities to restore capabilities or services that were impacted by the security incident.

E-Mail Policy:

E-mail use is addressed in Montague ISD's Acceptable Use Policy. A spam filter is in place to detect unsolicited and unwanted email and prevent those messages from getting to a user's inbox, and this spam filter is not to be removed or altered except by Montague ISD's IT. ABC ISD stresses that the following activities are prohibited by policy:
*Sending email that is intimidating or harassing.
*Using email for purposes of political lobbying or campaigning.
*Violating copyright laws by inappropriately distributing protected works.
*Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
*The use of unauthorized e-mail software.
*Excessive personal use. Personal Use of email is a privilege which is revocable at any time.

The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
*Sending or forwarding chain letters.
*Sending unsolicited messages to large groups except as required to conduct Montague ISD business.
*Sending or forwarding email that is likely to contain computer viruses.

In addition:

- All sensitive Montague ISD'S material transmitted over external network must be encrypted.
- All user activity on Montague ISD'S information resource assets is subject to logging and review.
- Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Montague ISD or any unit of Montague ISD unless appropriately authorized to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing Montague ISD. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."
- Individuals must not send, forward or receive confidential or sensitive Montague ISD information through non-Montague ISD email accounts. Examples of non-Montague ISD email accounts include, but are not limited to: Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

Individuals must not send, forward, receive or store confidential or sensitive Montague ISD information utilizing non-Montague ISD accredited mobile devices. Examples of mobile devices include, but are not limited to: Personal Data Assistants, two-way pagers and cellular telephones.

Malicious Code Policy:

The purpose of the Malicious Code Policy is to describe the requirements for dealing with computer virus, malware, spyware, worm and Trojan Horse prevention, detection and cleanup.

- The willful introduction of computer viruses or disruptive/destructive programs into the Montague ISD environment is prohibited, and violators may be subject to prosecution.
- All workstation systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to IT's recommendations.
- All servers that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Help Desk.
- All incoming data including electronic mail must be scanned for viruses where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.
- Where feasible, system or network administrators should inform users when a malicious code threat has been detected.
- Virus scanning logs should be maintained whenever email is centrally scanned for viruses.

Network Access Policy:

The purpose of the Montague ISD Network Access Policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of Montague ISD's information.

- Users are permitted to use only those network addresses issued to them by Montague ISD's IT.
- All remote access (dial in services) to Montague ISD will be either through an approved modem pool or via an approved Internet Service Provider (ISP) or VPN.
- Remote users may connect to Montague ISD'S information resources only through methods and using protocols approved by Montague ISD.
- Users inside the Montague ISD firewall may not be connected to the Montague ISD network at the same time remote access is being used to connect to an external network.

- Users must not install network hardware or software that provides network services without written approval from the IRM. This includes wireless access points, modems, and remote access software.
- Non-ABC ISD computer systems that require network connectivity must conform to Montague ISD IT Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, Montague ISD users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the ABC ISD network infrastructure without written approval from the IRM.
- Users are not permitted to alter network hardware in any way.

Password Policy:

Montague ISD has established the following rules for the creation, distribution, safeguarding, termination, and reclamation of Montague ISD user authentication.

- Stored passwords must be encrypted.
- User account passwords must not be divulged to anyone. Montague ISD's IT and IT contractors must not ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with Montague ISD.
- If the security of a password is in doubt, the password must be changed immediately.
- Administrators must not circumvent the Password Policy for the sake of ease of use.
- Users must not circumvent password entry with auto logon, application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Montague ISD's IT. In order for an exception to be approved there must be a procedure to change the passwords.
- Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
- IT Helpdesk password change procedures must include the following:
  *Authenticate the user to the helpdesk before changing password
  *Change to a strong password
  *The user must change password at first login
- In the event passwords are found or discovered, the following steps must be taken:
  *Take control of the passwords and protect them
  *Report the discovery to the Montague ISD IT Help Desk

Passwords must be "strong" in nature by using a minimum of eight characters and a combination of alpha and numeric characters. Passwords must be changed at least every 90 days.

Portable Computing Policy:

The purpose of this policy is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of Montague ISD's information. Portable computing devices are defined as any easily portable device that can receive and/or transmitting data to and from Montague ISD's information resources. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers, and cell phones.

- Only Montague ISD approved portable computing devices may be used to access Montague ISD's information resources.

- Portable computing devices must be password protected.
- Sensitive Montague ISD data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive Montague ISD data should be encrypted using approved encryption techniques.
- Montague ISD data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
- Montague ISD mobile devices including, but not limited to PDAs and smart phones will be used only for ABC ISD business and must be used in accordance with the guidelines of this document.
- All remote access (dial in services) to Montague ISD's network must be through an approved method as established in the network access policy.
- Non-Montague ISD computer systems that require network connectivity must conform to Montague ISD's IT Standards and must be approved in writing by the Montague ISD's IT. Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

All mobile devices must be password protected. Users must report lost or stolen mobile devices IMMEDIATELY. During normal business hours, the report should be made to the Montague ISD IT Help Desk. After normal business hours and on weekends, lost or stolen devices should be reported to the IT Director via his/her email.

Privacy Policy:

The purpose of this policy is to communicate the Montague ISD'S Information Technology privacy expectations to users.

- Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of Montague ISD are not private and may be accessed by Montague ISD IT employees, for business reasons at any time without knowledge of the information resource user or owner.
- To manage systems and enforce security, Montague ISD IT may log, review, and otherwise utilize any information stored on or passing through its IT systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. For these same purposes, the Montague ISD may also capture User activity such as IP addresses and web sites visited.
- A wide variety of third parties have entrusted their information to Montague ISD for business purposes, and all workers at Montague ISD must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential, and access will be strictly limited based on business need for access.
- Users must report any weaknesses (i.e. privacy incident breaches) in the Montague ISD computer security, any incidents of possible misuse or violation of this agreement to the proper authorities. An internal email address, Information Security, has been established within the Montague ISD'S for reporting information security issues. This email address is securityreporting@montagueisd.org.
- Users must not attempt to access any data or programs contained on the Montague ISD systems for which they do not have authorization or explicit consent.

Software Licensing Policy:

- Montague ISD provides enough licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.

- Third party copyrighted information or software, that the Montague ISD does not have specific approval to store and/or use, must not be stored on Montague ISD systems or networks. All software on Montague ISD computers and or servers will be procured, maintained and installed by IT unless specific written approval is granted. System administrators may remove unauthorized material.
- Third party software in the possession of Montague ISD must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.

Backup/Disaster Recovery Policy:

Montague ISD backups their data by utilizing the following: Offsite backup through PCNET.

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- The Montague ISD's Information Technology backup and recovery process for each system must be documented and periodically reviewed.
- The vendor(s) providing offsite backup storage for Montague ISD must be cleared to handle the highest level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest Montague ISD sensitivity level of information stored.
- A process must be implemented to verify the success of the Montague ISD's electronic information backup and then these backups must be periodically tested (at minimum every 6 months) to ensure that they are recoverable.
- Procedures must be reviewed at least annually.

Internet Content Filtering Policy:

In compliance with the Children's Internet Protection Act (CIPA) and Regulations of the Federal Communications Commission (FCC), the Montague ISD has adopted and will enforce this Internet safety policy that ensures the use of technology protection measures (i.e., filtering or blocking of access to certain material on the Internet) on all District computers with Internet access. Such technology protection measures apply to Internet access by both adults and minors with regard to visual depictions that are obscene, child pornography, or, with respect to the use of computers by minors, considered harmful to such students. The district will provide for the education of students regarding appropriate online behavior including interacting with other individuals on social networking Web sites and in chat rooms, and regarding cyberbullying awareness and response. At the present time Montague ISD utilizes Sonic Wall Content Filter monitored by PCNET for content filtering.

Further, the Board of Education's decision to utilize technology protection measures and other safety procedures for staff and students when accessing the Internet fosters the educational mission of the schools including the selection of appropriate teaching/instructional materials and activities to enhance the schools' programs; and to help ensure the safety of personnel and students while online.

However, no filtering technology can guarantee that staff and students will be prevented from accessing all inappropriate locations. Proper safety procedures, as deemed appropriate by the applicable administrator/program supervisor, will be provided to ensure compliance with the CIPA.

In addition to the use of technology protection measures, the monitoring of online activities and access by minors to inappropriate matter on the Internet and World Wide Web may include, but shall not be limited to, the following guidelines:

*Ensuring the presence of a teacher and/or other appropriate District personnel when students are accessing the Internet including, but not limited to, the supervision of minors when using electronic mail, chat rooms, instant messaging and other forms of direct electronic communications. As determined by the appropriate building administrator, the use of e-mail, chat rooms, as well as social networking Web sites, may be blocked as deemed necessary to ensure the safety of such students;
*Monitoring logs of access in order to keep track of the web sites visited by students as a measure to restrict access to materials harmful to minors;
*In compliance with this Internet Safety Policy as well as the District's Acceptable Use Policy, unauthorized access (including so-called "hacking") and other unlawful activities by minors are prohibited by the District; and student violations of such policies may result in disciplinary action; and
*Appropriate supervision and notification to minors regarding the prohibition as to unauthorized disclosure, use and dissemination of personal identification information regarding such students.

Incident Management Policy:

Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some the actions that can be taken to reduce the risk and drive down the cost of security incidents. Montague ISD will create and maintain a Computer Incident Response Team (CIRT). This team is responsible for coordinating the response to computer security incidents at the district including all cyber-security incidents. ISO referenced below refers to the Information Security Officer who will be appointed by the Superintendent of Montague ISD.

- Montague ISD's CIRT members have pre-defined roles and responsibilities which can take priority over normal duties.
- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
- The ISO is responsible for notifying the CIRT and initiating the appropriate incident management action including restoration of data.
- The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The appropriate technical resources from the CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The ISO, working with the Superintendent, will determine if a widespread Montague ISD communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to assess, eliminate or mitigate the vulnerability.
- The ISO is responsible for initiating, completing, and documenting the incident investigation.
- The Montague ISD's ISO is responsible for reporting the incident to the:
  *Superintendent
  *Department of Information Resources as outlined in TAC 202
  *Local, state or federal law officials as required by applicable statutes and/or regulations
- The ISO is responsible for coordinating communications with outside organizations and law enforcement.
- In the case where law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the Superintendent.

- In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement and the Montague ISD.

Intrusion Detection Policy:

Intrusion detection provides two important functions in protecting information resources:

*Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.

*Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

Montague ISD's Intrusion Detection Policy is outlined below:

- Intruder detection must be implemented for all servers containing data classified as high risk.
- Operating system and application software logging processes must be enabled on all critical server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems should be enabled.
- Server, firewall, and critical system logs must be reviewed frequently (at least monthly). Where possible, automated review should be enabled, and alerts should be transmitted to the administrator when a serious security intrusion is detected.
- Intrusion tools must be installed where appropriate and checked on a regular basis.

Network Configuration Policy:

The purpose of the Montague ISD's Network Configuration Security Policy is to establish the rules for the maintenance, expansion and use of the network infrastructure and to insure secure configuration management. These rules are necessary to preserve the integrity, availability, and confidentiality of Montague ISD's information.

- Montague ISD owns the network infrastructure and ABC ISD's IT is responsible for the network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
- To provide a consistent Montague ISD network infrastructure capable of exploiting new networking developments, all cabling must be installed by Montague ISD's IT or an approved contractor.
- All network connected equipment must be configured to a specification approved by Montague ISD's IT.
- All hardware connected to the Montague ISD's network is subject to the Montague ISD's IT management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of Montague ISD's IT.
- The Montague ISD's network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by Montague ISD's IT.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by Montague ISD's IT.
- All connections of the network infrastructure to external third-party networks are the responsibility of Montague ISD's IT. This includes connections to external telephone networks.
- Montague ISD's firewalls must be installed and configured to comply with all components of this plan.
- The use of departmental firewalls is not permitted without the written authorization from Montague ISD's IT.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Montague ISD's network without Montague ISD's IT approval.
- Users must not install network hardware or software that provides network services without Montague ISD's IT approval.
- Users are not permitted to alter network hardware in any way.

Physical/Environmental Access and Protection Policy:

The purpose of the Montague ISD's Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Technology facilities. All Montague ISD employees are responsible for adhering to this policy and with any local physical and environmental security requirements.

- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all Information Technology restricted facilities must be documented and managed.
- All IT facilities must be physically protected in proportion to the criticality or importance of their function.
- Access to IT facilities will only be granted to Montague ISD personnel and contractors whose job responsibilities require access to that facility.
- The process for granting card and/or key access to IT facilities must include the approval of the person responsible for the facility.
- Each individual who is granted access rights to an IT facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Technology facility. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for the IT facility immediately.
- Cards and/or keys must not have identifying information other than a return mail address.
- All IT facilities that allow access to visitors will track visitor access with a sign in/out log.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
- Card access records and visitor logs for IT facilities must be kept for routine review based upon the criticality of the information resources being protected. The person responsible for the IT facility must remove the card and/or key access rights of individuals that change roles within ABC ISD or are separated from their relationship with Montague ISD.
- Visitors must be escorted in card access controlled areas of IT facilities.
- The person responsible for the IT facility shall review access records and visitor logs for the facility on a periodic basis (at minimum once a month) and investigate any unusual access.
- The person responsible for the IT facility must review card and/or key access rights for the facility on a periodic basis (at minimum once a month) and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location.

Security Monitoring Policy:

The purpose of the Security Monitoring Policy is to ensure that Information Technology security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact.

- Automated tools will be used by the Montague ISD's IT to provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed, and the tools will report exceptions. These tools will be deployed to monitor:
  *Internet traffic
  *Electronic mail traffic

*LAN traffic, protocols, and device inventory
*Operating system security parameters

- The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
  *Automated intrusion detection system logs
  *Firewall logs
  *User account logs
  *Network scanning logs
  *System error logs
  *Application logs
  *Data backup and recovery logs
  *Help desk trouble tickets

- The following checks will be performed at least quarterly by assigned individuals:
  *Password strength
  *Unauthorized network devices
  *Unauthorized personal web servers
  *Unsecured sharing of devices
  *Operating System and Software Licenses

Any security issues discovered will be reported for follow-up investigation.

System Security Policy:

All systems introduced on the Montague ISD's network must be made secure before placing them into production. This is known as "hardening" the systems. This process should be a combination of vendor recommendations, and industry best practices and procedures as deemed appropriate. Montague ISD will do this by adhering to the following:

- Installing the operating system from an IT approved source.
- All systems connected to the Montague ISD network should have a vendor supported version of the operating system installed.
- All systems connected to the Montague ISD network must be current with security patches, hot fixes or updates for operating systems and applications. Security patches, hot fixes or updates must be applied in a timely manner, as approved by IT, to protect Montague ISD's information resources.
- Setting security parameters, file protections and enabling audit logging.
- Warning banners must be established, as appropriate, on all system access points.
- All unnecessary services should be disabled.
- Systems in the final stages of hardening may be placed on the Montague ISD network in an isolated segment such as a segmented lab environment to minimize exposure.
- Vulnerability scans or penetration tests must be performed on all Internet-facing applications and systems before placement into production. At a minimum, quarterly audits must be conducted to re-evaluate the risk potential of applications and systems.
- System integrity checks of server systems housing high risk ABC ISD data must be performed quarterly.

Security Systems Management Policy:

The term "security systems" as used in this policy is defined as any singular system or any combination of the systems including but not limited to: Access control systems enable the monitoring and control of access to

facilities and resources; Hold-up and/or Panic Alarm that signal administrators of an event in which the personal safety of a member of the district is in jeopardy; Intrusion Detection Systems commonly referred to as "burglar alarms"; and security cameras. Security systems are installed for the protection of our students, employees and visitors. Therefore, security systems may not be removed, relocated, or modified without approval of the Superintendent, or his/her designee.

*All security systems must be approved by the Superintendent, or the Superintendent's designee, prior to purchase and installation.

*Upon installation of a security system, building level principals, or their designee, will monitor the system. Stand-alone security systems (those not monitored by the district) are prohibited.

*For the purposes of security and potential evidence gathering, it is important that any audio or video recorded from security systems be protected. Any department that has video and/or audio surveillance equipment installed shall provide the Superintendent, or their designee, with the appropriate authorization to view, download, capture, monitor, and control this equipment. This enables the Montague ISD to maintain a chain of custody regarding evidence recovered from the recording device.

*Security camera recordings should be retained for a period of no less than 14 days. If existing systems do not provide for a storage period of that length, the maximum storage period possible should be utilized.

Information Asset Inventory:

An Information Asset Inventory is one of the most crucial information assurance principles. Every single asset in the Montague ISD's data processing infrastructure must be accounted for and listed. Included in the listing should be document serial numbers, version, location, format, description, value and any another other data set that enhances understanding. Also, each class of document should contain a data classification as identified in the Data Classification Policy. It determines the level of protection the document(s) should receive.

Cloud Usage and Security Policy:

Cloud computing offers a number of advantages including low costs, high performance and quick delivery of services. However, without adequate controls, it also exposes individuals and organizations to online threats such as data loss or theft, unauthorized access to corporate networks, and so on. This cloud computing policy is meant to ensure that cloud services are NOT used without the IT's knowledge. It is imperative that employees NOT open cloud services accounts or enter into cloud service contracts for the storage, manipulation or exchange of company-related communications or company-owned data without the IT's input. This is necessary to protect the integrity and confidentiality of Montague ISD's data and the security of the network.

*Use of cloud computing services for work purposes must be formally authorized by the IT. The IT will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.

*For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the IT. The IT will decide what data may or may not be stored in the Cloud.

*The use of such services must comply with Montague ISD's existing Acceptable Use Policy/Computer Usage Policy/Internet Usage Policy/BYOD Policy.

*Employees must not share log-in credentials with co-workers. The TMT will keep a confidential document containing account information for continuity purposes.

*The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, school financial data, student identifiable information, or any other data owned or collected by Montague ISD.

*Personal cloud services accounts may not be used for the storage, manipulation or exchange of ISD-related communications or ISD-owned data.

Vendor/Third Party Access Policy:

- Vendors must comply with all applicable Montague ISD policies, practice standards and agreements, including, but not limited to:
  - *Safety Policies
  - *Privacy Policies
  - *Security Policies
  - *Auditing Policies
  - *Software Licensing Policies
  - *Acceptable Use Policies

- Vendor agreements and contracts must specify:
  - *The Montague ISD information the vendor should have access to
  - *How Montague ISD's information is to be protected by the vendor
  - *Acceptable methods for the return, destruction or disposal of Montague ISD's information in the vendor's possession at the end of the contract
  - *The Vendor must only use Montague ISD information and information resources for the purpose of the business agreement
  - *Any other Montague ISD information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others

- Montague ISD will provide an IT point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.
- Each vendor must provide the Montague ISD with a list of all employees working on the contract. The list must be updated and provided to Montague ISD within 24 hours of staff changes.
- Each on-site vendor employee must acquire a Montague ISD identification badge that will be displayed at all times while on Montague ISD premises. The badge must be returned to the Montague ISD when the employee leaves the contract or at the end of the contract.
- Each vendor employee with access to Montague ISD sensitive information must be cleared to handle that information.
- Vendor personnel must report all security incidents directly to Montague ISD's IT.
- If vendor management is involved in Montague ISD's security incident management, the responsibilities and details must be specified in the contract.
- Vendor must follow all applicable Montague ISD's change control processes and procedures.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate Montague ISD management.

Change Management Policy:

The purpose of this policy is to manage changes in a well-communicated, planned and predictable manner that minimizes unplanned outages and unforeseen system issues.

The following general requirements shall be met in the change management process:

- Scheduled change calendars and departmental communications operational procedures shall be developed to inform stakeholders of upcoming application and system changes that impact system availability or operations.
- Regular planned changes shall minimally be communicated to all stakeholders on a monthly basis through a communication mechanism of the Montague ISD's choosing.
- Unplanned outages shall be communicated immediately to stakeholders with regular updates on progress towards resolution and resumption of service.
- Regular system and application patching schedules shall be communicated to users and performed in such a way as to minimize system downtime and user productivity.
- Changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) shall to be reported to or coordinated with stakeholders and shall be notified through a communication mechanism of the Montague ISD's choosing.
- Device configurations shall be backed up and rollback procedures must exist prior to implementing a change.